(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 300 997 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.04.2003 Bulletin 2003/15

(51) Int Cl.[7]: **H04L 12/58**

(21) Application number: **02254884.6**

(22) Date of filing: **11.07.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **06.10.2001 KR 2001061649**
29.05.2002 KR 2002029828

(71) Applicant: **Terrace Technologies, Inc.**
Sungdong-gu, Seoul 133-821 (KR)

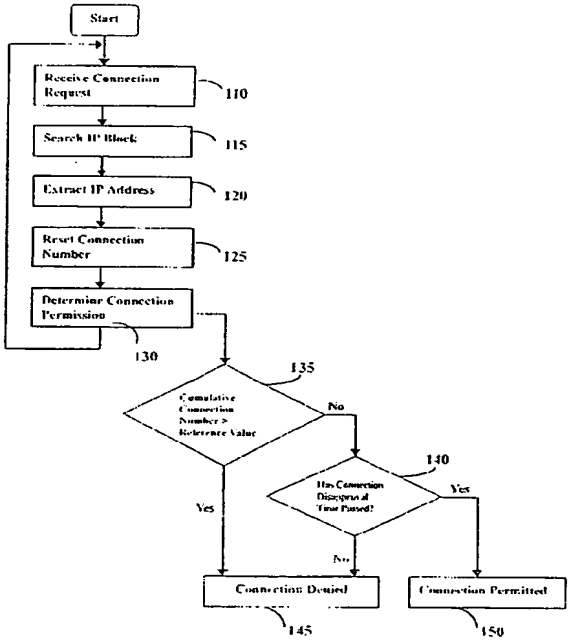
(72) Inventors:
- **Lim, Sung-Yeop**
  Jungnang-ju, Seoul 131-120 (KR)
- **Lee, Woo-Joo**
  Gwangjin-gu, Seoul 143-222 (KR)

(74) Representative: **Findlay, Alice Rosemary**
Lloyd Wise
Commonwealth House,
1-19 New Oxford Street
London WC1A 1LW (GB)

(54) System and method for preventing unsolicited e-mail

(57) A connection request from a remote host is denied by an email service system, if the number of connection requests from the remote host exceeds a predetermined reference number, and the responsibility to re-send the denied email is transferred to the requesting host. For the determination of connection permission or denial, the number of connection requests from the remote host is calculated with reference to a corresponding IP address. By the IP filtering scheme, email traffic can be effectively managed and controlled. The email service system of the present invention includes a dynamic IP filtering module, a mail transfer agent (MTA), a receiving means for accepting a connection request from a remote host, a means for extracting an IP address corresponding to the requesting remote host according to an IP block, and a means for determining permission of connection by comparing a predetermined reference value with a summation value of the number of past requests made during a predetermined control time period and the current request from the extracted IP address, wherein the predetermined control time period is divided into a number of slices, and the dynamic filtering module includes a means for resetting, before the determination of connection permission, the number of connection requests in the slice(s) between the previous connection request time and the current time.

FIG. 3



EP 1 300 997 A2

Description

[0001] This invention relates generally to electronic mail service system and method, and more particularly to a dynamic IP filtering technology that adopts a varying start time conception to continuously filter IP addresses, apply multiple IP filtering policies and implement various IP filtering policies to a single IP group according to time.

[0002] Distributed computer networks such as the Internet are increasing global communication for information exchange and dissemination, and peer-to-peer communication using an electronic mail (email) system has become a daily business. Email is a widely used network application in which text messages are transmitted electronically between end users over various types of networks using various network protocols. The email system is a distributed client/server system having equivalent servers for providing email services to the clients. The email system is based on an open system where the clients communicate with the server to transmit and receive an email message and the server communicates with other servers. This open nature exposes the problems of ever increasing UCE (Unsolicited Commercial Email) such as spam mails, junk mails, email bombs and the like (referred to herein collectively as 'spam mail').

[0003] Since the 1990s, with the rise in commercial awareness of the Internet, spam mails have been used to indiscriminately send large amounts of unsolicited email messages for the purpose of commercial advertisement at lower cost. Spam mail has become a serious threat to both the ISPs (Information Service Providers) and end users. The ISPs waste their system resources in dealing with the spam mail network resources in transmitting spam messages of more than several giga byte targeted to over hundred thousands users, and additional communications costs and the loss of system and human resources in taking counter-measures, e.g., automatic returning the spam mail to the sender and processing refusal or complaint messages from the spam recipients. Likewise, many receivers pay for the time to distinguish actual mail from the spam mail and waste computing resources.

[0004] Conventional methods to solve the spam mail threat include a recipient approach and an email service provider approach. This server-based solution is a combination of a MTA control technology and a contact regulation in which a spam sender is prohibited from using anonymous configurations and the relay of SMTP (Simple Mail Transfer Protocol) is blocked.

[0005] Generally, mail server traffic in an ISP is 5 to 10 times more in receiving email than in transmitting email, and spam mail amounts to about 60 to 80% of the receiving mail traffic. Many spammers hide behind false retum addresses and deliberately write messages to mislead recipients. Therefore, the most reliable method to prevent spam mail may be reading and reviewing one by one the titles and body texts of mail messages to determine if the mail is spam. However, this takes too much time and costs both to the ISPs and end users, and determination of spam mail is difficult since the criteria of the determination is subjective.

[0006] Therefore, technical measures are needed on behalf of the Internet and email communities to more effectively solve the problems of spam mails.

SUMMARY OF THE INVENTION

[0007] An object of this invention is to minimize the loss of email service providers due to spam mail.

[0008] Another object of this invention is to effectively maintain and control the traffic of spam mail in the email service providers and to prevent damages from spam mail.

[0009] Yet another object of this invention is to provide an email service system and method that can apply separate spam blocking policies to IP (Internet Protocol) groups that request a connection to the system and can flexibly apply various IP filtering or blocking policies to a single IP group.

[0010] According to one aspect of the present invention, a connection request from a remote host is denied by an email service system, if the number of connection requests from the remote host exceeds in a predetermined reference number, and the responsibility to resend the denied email is transferred to the requesting host. For the determination of connection permission or denial, the number of connection requests from the remote host is calculated with reference to a corresponding IP address. By the IP filtering scheme, traffic of the email service system can be effectively managed and controlled.

[0011] The email service system of the present invention includes a dynamic IP filtering module, a receiving means for accepting a connection request from a remote host, a means for extracting an IP address corresponding to the requesting remote host according to an IP block, and a means for determining permission of connection by comparing a predetermined reference value with a summation value of the number of past requests made during a predetermined control time period and the current request from the extracted IP address wherein the predetermined control time period is divided into a number of slices. The dynamic filtering module includes a means for resetting, before the determination of connection permission, the number of connection requests in the slice(s) between the previous connection request time and the current time. A dynamic IP filtering method for an email services system comprises the steps of: receiving a connection request from a remote host; searching an IP block and extracting an IP address corresponding to the requesting remote host from the IP block; determining a connection permission by comparing a predetermined reference value with a summation value of the number of past requests made during a predetermined control time period and current request

from the extracted IP address; wherein the pre-determined control time period is divided into a number of slices, and resetting, before the determination step, the number of connection requests in the slice(s) between the previous connection request time and the current time.

[0012] According to other aspects of the present invention, various IP filtering policies may be applied to different IP groups or to a single IP group according to time, so that the traffic within the email service system can be controlled more effectively and the dynamic IP filtering technology is implemented more flexibly in diverse circumstances.

[0013] The invention will now be described by way of example with reference to the accompanying drawings in which:

Figs. 1 is a block diagram of overall configuration of an electronic mail network according to the present invention;

Fig. 2 is a schematic diagram for showing IP blocks and recorders in an electronic mail service system of the present invention;

Fig. 3 is a flow chart of the processes of a dynamic IP addresses filtering method in the electronic mail service system;

Fig. 4 is a block diagram for showing multiple policy technology applied to different IP blocks with different IP blocking policies according to the present invention;

Fig. 5 is a block diagram for illustrating an embodiment in which different IP filtering policies are applied to a single IP group according to time; and

Fig. 6 is a block diagram of an email service system implemented in a form of ASP (Application Service Provider).

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0014] Fig. 1 shows a configuration of the electronic mail network according to the present invention. The email network is a distributed computer system for generating, accessing, transmitting and receiving email and based on protocols including but not limited to IMAP (Intemet Messaging Access Protocol), POP (Post Office Protocol) and SMTP (Simple Mail Transfer Protocol).

[0015] A remote host 10 is connected to the email service system 100 through a network including a public network such as the Internet and LAN (Local Area Network). The remote host 10 may be an individual user client system or include a server system equivalent to the email service system 100. The network has plenty of connection nodes and communication is performed by using Internet Protocol (IP). The IP is widely known as a standard to communicate data. Upper layer protocols such as HTTP (HyperText Transfer Protocol) and FTP (File Transfer Protocol) communicate on an application layer, while lower layer protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol) undertake communications on transport and network layers. Mail messages are sent to the address e.g. <receiver@terracetech.com> using the SMTP protocol.

[0016] The email service system 100 includes one or more server computers and may configure a part of private intranet connected to the public network. For security, the communications between the public network and private intranet may be filtered and controlled by a firewall. The firewall restricts outsiders from accessing to a certain resources within the intranet. The server computer included in the email service system 100 is configured to execute server software programs on behalf of clients. The server computer is configured to maintain user accounts, to receive and organize mail messages so that they can readily be located and retrieved, no matter how the information in the message is encoded. The server computer may include a web server, CGI (Common Gateway Interface) programs, an account manager and SMTP mail server.

[0017] The email service system 100 comprises a dynamic IP address filtering module 20 and a mail transfer agent (MTA) 50 such as Sendmail™ and Qmail™. The MTA 50 includes a transfer MTA, a receiver MTA and a gateway MTA. The filtering module 20 comprises a connection processing unit 30 and an IP block 40. The email service system 100 receives new email messages using e.g. POP-3 protocol from the remote host 10 and transmits email messages by using SMTP (Simple Mail Transfer Protocol) or ESMTP (Extended SMTP) protocols.

[0018] The remote host 10 sends to the service system 100 a connection request and transfers to the service system 100 an email message, a file to be attached to the message and data necessary for transmitting the email messages e.g. MAIL From <spam@host.domain>, RCPT To <receiver@host.domain>. The connection processing unit 30 of the dynamic IP address filtering module 20 determines a permission of connection to the request from the remote host 10 with reference to the IP block 40. If connection is permitted, data and message transmitted from the remote host 10 are delivered to the MTA 50 and transferred to the designated email receiver or another remote host. The determination of the connection permission to the remote host 10 depends on the comparison result of reference value with the number of connection requests based on the IP address from a certain remote host, which will be explained in detail below.

[0019] Fig. 2 is conceptual diagram of configuration of the IP block and recorders in the email service system according to the present invention. The IP block in the email service system 100 is data stored in advance. When a remote host 10 requests a connection, an IP address associated to the remote host is recorded. The IP block 40 includes a plurality of IP groups 40a, 4Db, ···, 40k which are arranged according to a predeter-

mined rule of IP address grouping. The connection processing unit 30, receiving the connection request from a remote host 10, searches and extracts from the IP block 40 an IP address corresponding to the requesting remote host. It is preferable to configure the IP block of IP addresses by using e.g. a hash function, so that the connection permission can be determined with respect to concurrent plural connection requests. A single IP group (e.g. 40a) consists of a plurality of recorders (#0 ~ #m-1), and one recorder is formed to one IP address. Each of the recorders consists of a number of slices, e.g. 'n' slices from 'slice 0' to 'slice n-1'. The slice is a unit dividing the recorder based on time. In each of the slices, the number of connection request received from a certain remote host is recorded.

[0020] Fig. 3 shows the processing flow of the dynamic IP address filtering in an email service system of the present invention.

[0021] A connection request from a remote host is received at step 110. An IP address of the requesting remote host is extracted at step 120 by searching the IP block at step 115. Permission of connection of the remote host is preliminarily determined at step 130 based on cumulative number of requests from the extracted IP address. The determination is made at step 135 by examining if the total summation of requests exceeds a reference value. Here, the total summation request is obtained by adding the current request and cumulative number of requests that are recorded in the slices corresponding to time ranging from the nearest past connection requesting time (i.e. the previous requesting time) to the current request to time retroactive to a predetermined control period. For instance, suppose that a single recorder has ten slices, these slices are controlled in ten-minute time unit, the current request is received at 12:13, and the previous requesting time is 12:11. Among data recorded in the entire slices 0-9, the number of connections stored in slices 3-9 (i.e. slices corresponding to time between 12:03 to 12:10), the number of connection recorded in slice 0 (i.e. slice corresponding to time between 12:10 to 12:11) and the current connection request are summed to be the cumulative number of requests, and at step 135 the cumulative value is compared with the reference value. The reference value is determined by synthetically considering system resources of the email service provider, dimension of users, and traffic and denoted as the number of request per time.

[0022] If the cumulative connection number exceeds the reference value, the connection of the remote host corresponding to the associated IP address is denied at step 145. Even when the cumulative number of requests from a remote host does not exceed the reference value, it is determined that a connection disapproval time to the associated IP address has passed at step 140. When the connection disapproval time has not passed, the connection of the remote host corresponding to associated IP address is denied. If the connection disapproval time is passed or there have been no precedent cases to deny the connection, the connection is permitted at step 150 and email message and data are transferred to the MTA 50 to carry out normal email transmission process.

[0023] Prior to the determination of connection permission 130, the connection number is reset at step 125. The reset step of the connection number 125 resets the number of connection in slices between the previous connection time and current time to be '0'. In case of the example above, between slices corresponding to the previous requesting time 12:11 and the current time 12:13 there exists a slice to 12:02. This is because there is no connection between the previous connection time and current time and thus in this time interval connection number data is recorded in slice(s) corresponding to past time prior to time retroactive to the slice control time (in this instance ten minutes). Accordingly, the connection time data stored in the past slice is reset to '0' so that the control time can be maintained as continuous time value.

[0024] After the determination step of connection permission 130, the sequence flows back to the receiving step of new connection request 110. It may be considered to memory the IP address to which the connection is permitted and to omit the searching IP block to the identical IP address. However, in view of system resources to memory or store the IP address data in connection with the connection permission, it is preferable to search the IP block and extract corresponding IP address whenever a connection is requested.

[0025] In use of the dynamic IP filtering technique, multiple time policies can be applied to a single data structure.

[0026] Fig. 4 is a block diagram illustrating the multiple time policies by which different policies are applied to each of the plural of IP blocks. IP filtering policy A 200a applied to IP group A 40a has different unit control time, reference value and connection disapproval time from those of policies B and C 200b and 200c. At this time, the 'unit control time' means the period of time used for summing the requested number at step 135 of Fig. 3, and the 'reference value' refers the reference number compared with the summation of cumulative number of request during the unit control time and the current request. The multiple IP filtering policy has, for instance, the unit control time a1 of one hour, the reference value 12 of 10 times, and the connection disapproval time a3 of two hours to an IP group A 40a having IP addresses from 210.220.10.0 to 20.220.250.255, while an IP group B 40b of IP addresses ranging from 210.0.10.0 to 210.220.0.0 is subject to IP filtering policy B 200b which has the unit control time b1 often minutes, the reference value b2 of 10 times, and the connection disapproval time b3 of thirty minutes. In the multiple IP filtering policy, a default policy may be applied to IP groups that does not need a special policy. When it is required to confirm if a certain IP address is to be blocked, parameters in

associated IP filtering policy to the IP group including the certain IP address may be called and read. The policy parameters (e.g. unit control time, reference value, and connection disapproval time) are applied to the associated IP filtering policy and calculated.

[0027] As shown in Fig. 5, different policies may be applied to a single IP group 40n according to time. By doing this, it is possible to apply dynamically and flexibly a specially reinforced policy to a certain time period when requests for spam mails are peak and thus more efficient management of server traffic is made possible.

[0028] Fig. 6 is a block diagram of an email service system implemented in a form of ASP (Application Service Provider). The email service system 210 receives a connection request, a signal necessary for transmission of email message, an email message and file attached to the message, and the dynamic IP filtering module 220 determines the permission of connection to the request from a remote host 10. When the connection is permitted, the email service system 210 transfers the email message and necessary data to a plurality of remote servers 300a. 300b and 300c interconnected via a communication network 400. The dynamic IP filtering module 220 includes, like the system 100 of Fig. 1, a connection processing unit 230 and an IP block 240. The remote servers 300a, 300b and 300c has their own MTA 250a, 250b and 250c, which may include a transfer MTA, receiving MTA and gateway MTA.

[0029] In the ASP implementation of the email service system of the present invention, each of the remote servers 300a, 300b and 300c can utilize outside resources of IP filtering module and thus can save their own system resource.

Claims

1. An email service system having a dynamic filtering module and comprising means for receiving a connection request from a remote host, means for extracting an IP address corresponding to the requesting remote host according to an IP block, and means for determining permission of connection by comparing a predetermined reference value with a summation value of the number of past requests made during a predetermined control time period and the current request from the extracted IP address, wherein the predetermined control time period is divided into a number of slices, and wherein the dynamic filtering module including means for resetting, before the determination of connection permission, the number of connection requests in the slice(s) between the previous connection request time and the current time.

2. The email service system of Claim 1, wherein a connection disapproval time is established for the IP address when the determination means denies the connection, and connection of the IP address is blocked until the connection disapproval time passes.

3. The email service system of Claim 2, wherein the IP block includes a plurality of IP groups and an IP filtering policy applied to one IP group is different from that applied to other IP groups, each IP filtering policy including data for the predetermined control time, the reference value and parameters related to the connection disapproval time.

4. The email service system of Claim 2, wherein the IP block includes a plurality of IP groups, and plural IP filtering policies are applied to a single IP group, each policy induding data for the predetermined control time period, the predetermined reference value and parameters related to the connection disapproval time.

5. The email service system of any preceding claim and interconnected to a plurality of remote servers via a communication network, the remote servers each having a mail transfer agent (MTA), the email service system further comprising means for transferring to a corresponding remote server an email for which connection is permitted by the determination means.

6. A method for dynamically filtering an IP address in an email service system, the method comprising receiving a connection request from a remote host; searching an IP block and extracting an IP address corresponding to the requesting remote host from the IP block, determining a connection permission by comparing a predetermined reference value with a summation value of the number of past requests made during a predetermined control time period and the current request from the extracted IP address, wherein the predetermined control time period is divided into a number of slices, and resetting, before the determination step, the number of connection requests in the slice(s) between the previous connection request time and the current time.

7. The method of Claim 6, wherein a connection disapproval time is established for the IP address when the determination means denies the connection, and connection of the IP address is blocked until the connection disapproval time passes.

8. The method of Claim 7, wherein the IP block includes a plurality of IP groups and an IP filtering policy applied to one IP group is different from that applied to other IP group, each IP filtering policy including the predetermined control time period, the predetermined reference value and parameters related to the connection disapproval time.

9. The method of Claim 7, wherein the IP block includes a plurality of IP groups and a plurality of IP filtering policies are applied to a single group, each IP filtering policy including the predetermined control time period, the predetermined reference value and parameters related to the connection disapproval time.

10. The method of any one of Claims 6 to 9, wherein the IP block including recorders each corresponding to one IP address, each of the recorders comprising a plurality of slices continuously managed according to the predetermined control time period, and to each of the recorders is written the number of connection requests of the corresponding IP address

11. The method of any one of Claims 6 to 10, wherein, after the determination step, the sequence returns to the step of receiving a connection request from a remote host.

12. The method of any one of Claims 6 to 11 wherein the email service system is connected to a plurality of remote servers each of which has its own mail transfer agent, the method further comprising transferring an email associated with the remote host for which connection is permitted by the determination step to the corresponding remote server.

FIG. 1

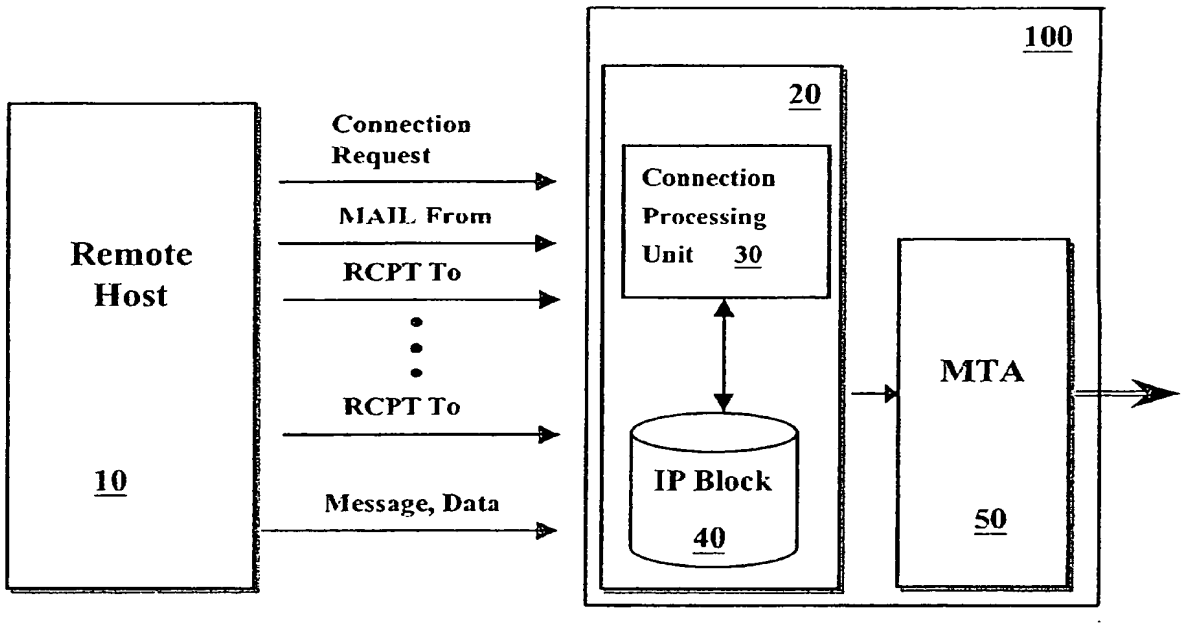


FIG. 2

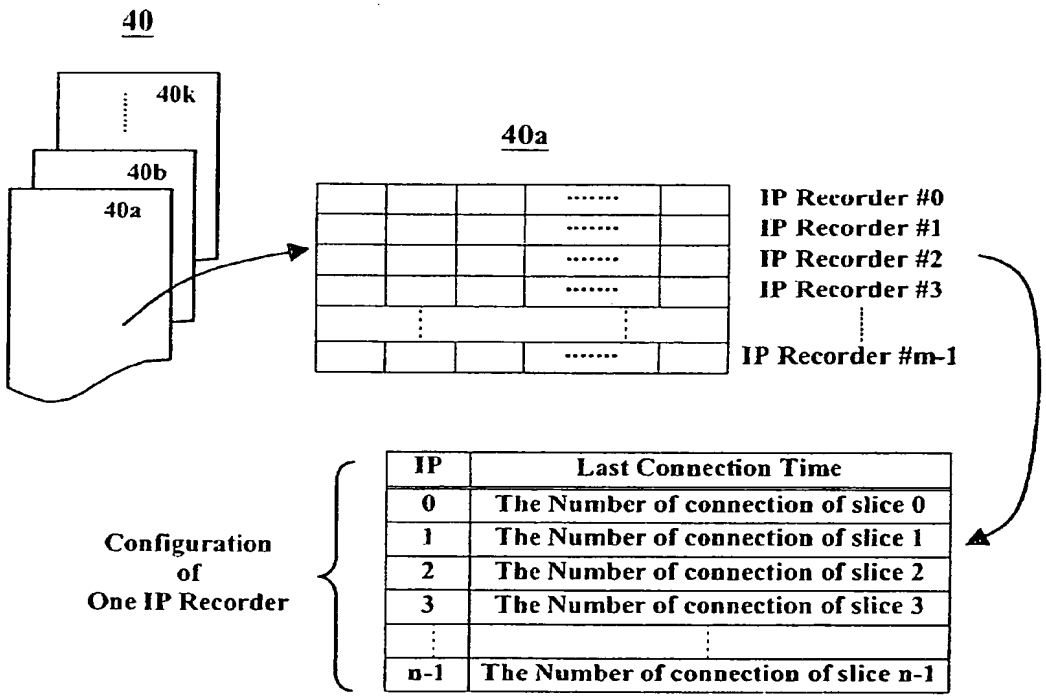


FIG. 3

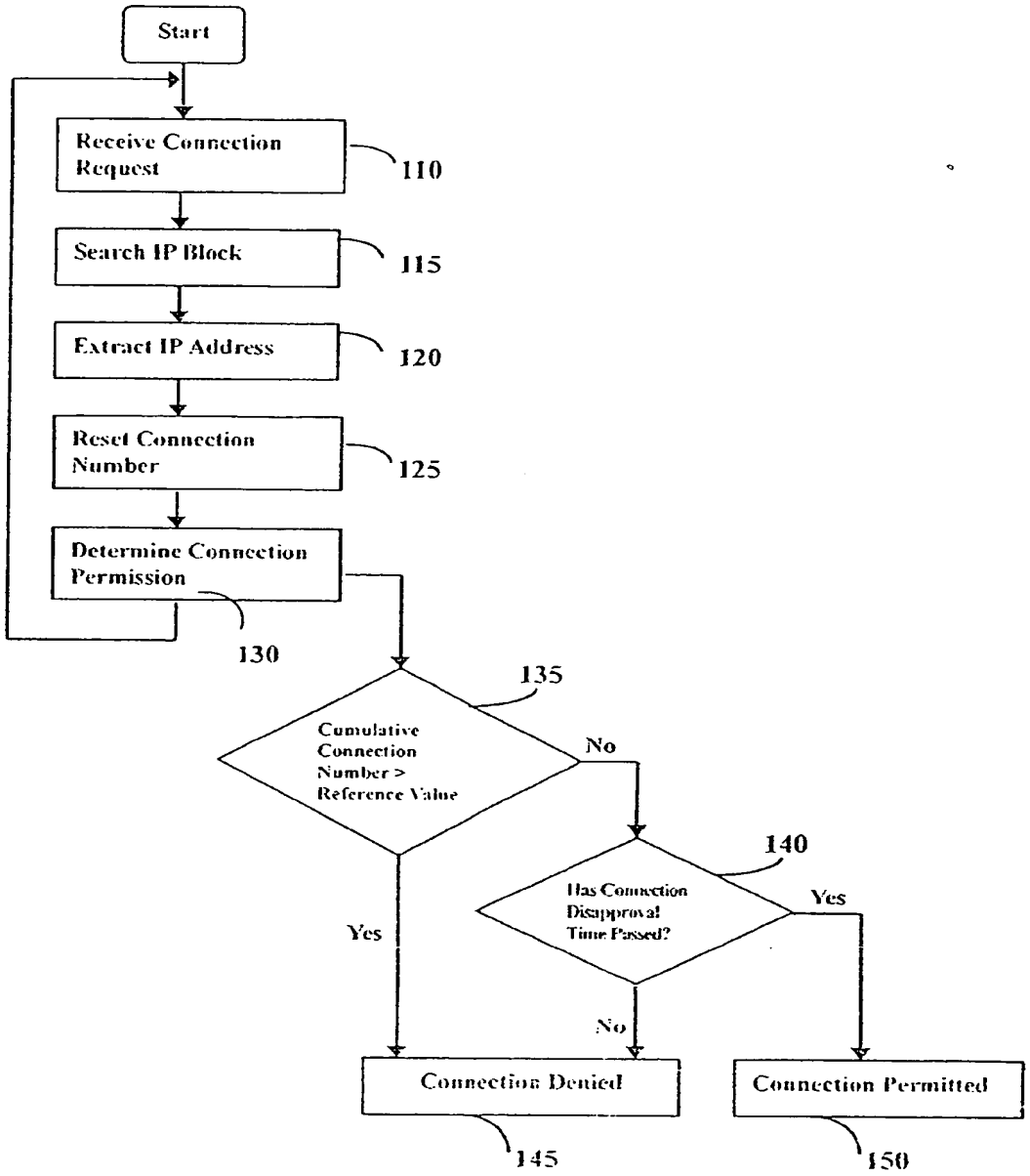


FIG. 4

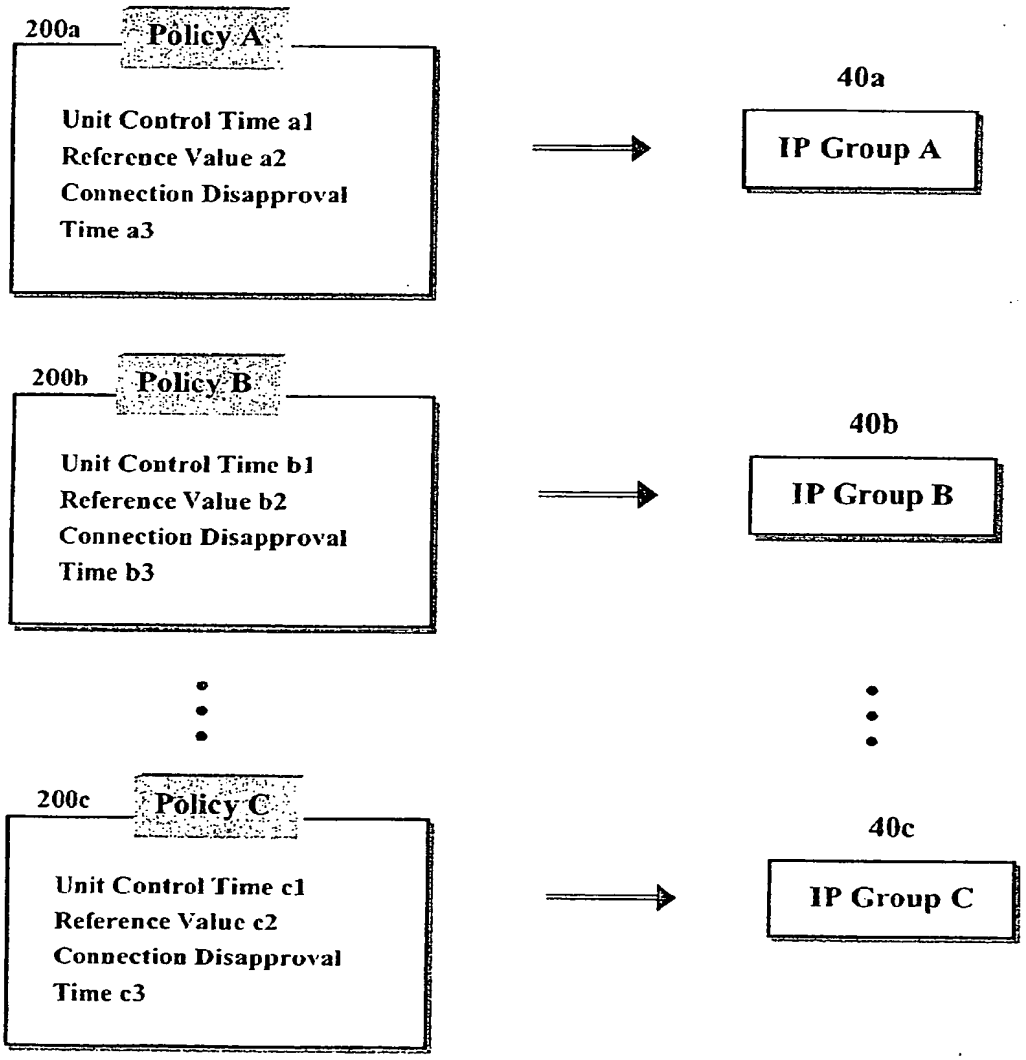


FIG. 5

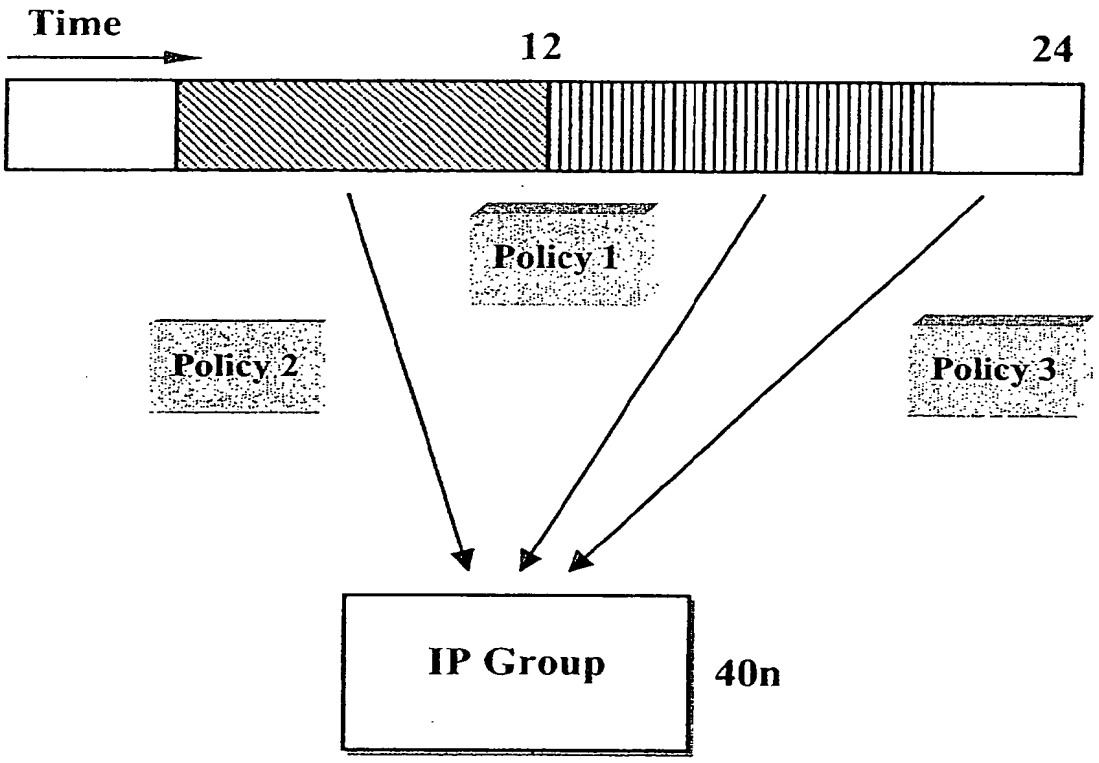
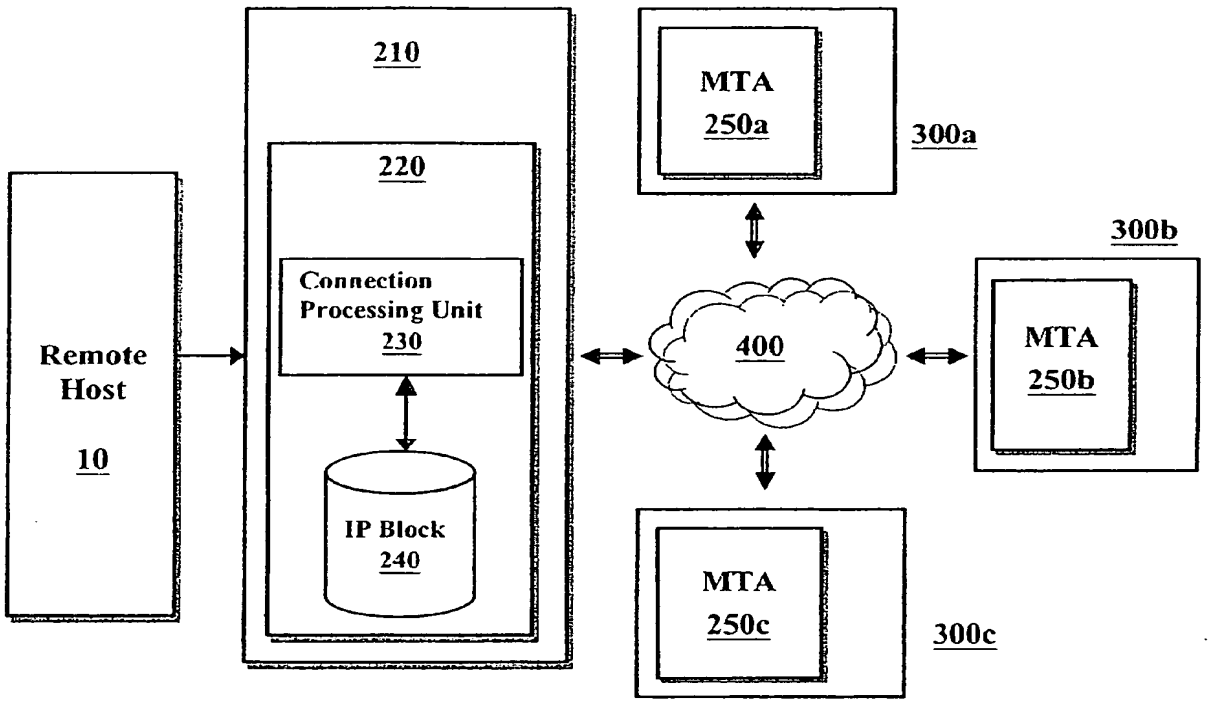


FIG. 6



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 300 997 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
02.01.2004 Bulletin 2004/01

(43) Date of publication A2:
09.04.2003 Bulletin 2003/15

(21) Application number: **02254884.6**

(22) Date of filing: **11.07.2002**

(51) Int Cl.[7]: **H04L 12/58**, H04L 29/06

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **06.10.2001 KR 2001061649**
29.05.2002 KR 2002029828

(71) Applicant: **Terrace Technologies, Inc.**
Sungdong-gu, Seoul 133-821 (KR)

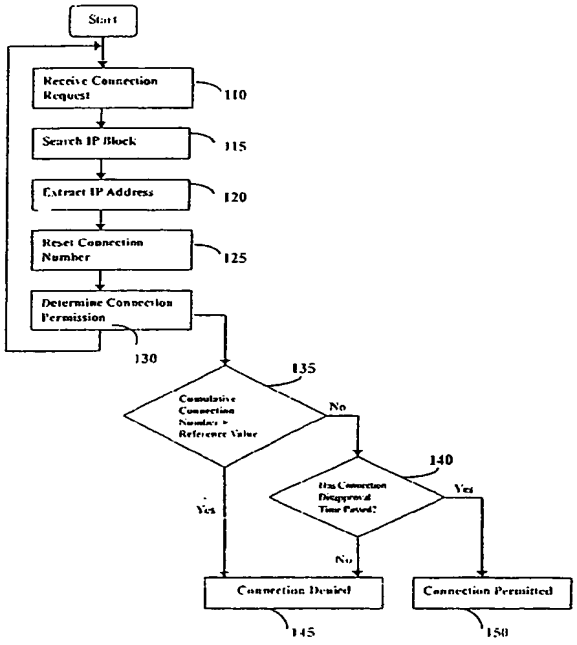
(72) Inventors:
- **Lim, Sung-Yeop**
  Jungnang-ju, Seoul 131-120 (KR)
- **Lee, Woo-Joo**
  Gwangjin-gu, Seoul 143-222 (KR)

(74) Representative: **Findlay, Alice Rosemary**
Lloyd Wise
Commonwealth House,
1-19 New Oxford Street
London WC1A 1LW (GB)

(54) System and method for preventing unsolicited e-mail

(57) A connection request from a remote host is denied by an email service system, if the number of connection requests from the remote host exceeds a predetermined reference number, and the responsibility to re-send the denied email is transferred to the requesting host. For the determination of connection permission or denial, the number of connection requests from the remote host is calculated with reference to a corresponding IP address. By the IP filtering scheme, email traffic can be effectively managed and controlled. The email service system includes a dynamic IP filtering module, a receiving means for accepting a connection request from a remote host, a means for extracting an IP address corresponding to the remote host, and a means for comparing a predetermined reference value with a summation value of the number of past requests made during a predetermined control time period and the current request from the extracted IP address.

FIG. 3



EP 1 300 997 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 25 4884

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 6 189 035 B1 (LOCKHART THOMAS WAYNE ET AL) 13 February 2001 (2001-02-13) * column 1, line 25 - column 1, line 44 * * column 3, line 11 - column 5, line 11 * * claims 1,2 *	1-12	H04L12/58 H04L29/06
A	EP 0 909 072 A (LUCENT TECHNOLOGIES INC) 14 April 1999 (1999-04-14) * page 2, line 35 - page 3, line 3 * * page 4, line 1 - page 5, line 2 *	3,4,8,9	
A	WO 01 38999 A (ESCOM CORP ;DONALDSON ALBERT L (US)) 31 May 2001 (2001-05-31) * page 37, line 15 - page 38, line 10 *	2,7	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	21 October 2003	Gavriliu, B-A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 25 4884

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-10-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6189035 B1	13-02-2001	CN 1308745 T	15-08-2001
		EP 1088261 A1	04-04-2001
		WO 9959071 A1	18-11-1999
EP 0909072 A	14-04-1999	US 6141749 A	31-10-2000
		EP 0909072 A2	14-04-1999
		JP 11163940 A	18-06-1999
		JP 2003198637 A	11-07-2003
WO 0138999 A	31-05-2001	US 6321267 B1	20-11-2001
		AU 1783501 A	04-06-2001
		CA 2392397 A1	31-05-2001
		EP 1234244 A1	28-08-2002
		WO 0138999 A1	31-05-2001

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82